REMARKS

Claims 1-11 are all the claims pending in the application.

In the Final Office Action dated April 20, 2005, claims 1 – 3 and 5 – 11 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Mittra (U.S. Patent No. 5,748,736) in view of Roden (U.S. Patent No. 5,970,477). Further, claims 1, 4 and 7 – 11 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wesley et al. (U.S. Patent No. 6,275,859 B1) in view of Roden.

These rejections are respectfully traversed.

The present invention, as expressed by claim 1, for example, relates to a multicast system including a sender terminal for transmitting multicast data, a receiver terminal for receiving multicast data, an authentication server processor for managing the sender terminal and the receiver terminal, a first user processor provided in the sender terminal for transmitting a login requirement to the authentication server processor, and a second user processor provided in the receiver terminal for transmitting a login requirement to the authentication server processor.

The independent claims were previously amended to relate the claimed invention to the features that (1) an encryption key is periodically generated by the authentication server processor and transmitted to the receiver terminals, and (2) the authentication server processor executes a logout when the second user processor in a receiver terminal does not receive the periodically distributed encryption key.

These features are described in detail in the specification at page 11. To summarize, a common key, in which the digital signature is written by the secret key in the authentication server terminal, is encrypted using the public key of the user, and the encrypted common key and transmitted to the user. Next, an encryption key encrypted using the common key is transmitted to the user. This is done on a periodic basis. The periodic transmission of the encryption key is effected in order to prevent the encryption key from being illegally obtained and used.

If the key update controller (231) of the authentication server terminal receives an acknowledgement receipt of the key from the user, this result is stored in the server management information (250) and the process repeats. However, if the key update controller (231) does not receive the acknowledgement receipt of the key from the user within a predetermined time, the key update controller regards this as indicative of the fact that the user has terminated receiving keys transmitted from the authentication server terminal, causing a logout process to be executed.

These features of the invention are by no means taught or suggested by the combination of Mittra or Wesley with Roden.

The Examiner relies in both cases on Roden to supply these features. Specifically, the Examiner points to column 17, lines 35 – 39, of Roden which state:

> If the received message does not include[] the correct key, the "NO" branch is followed to step 605 in which the point of presence 22 responds to a potential fraudulent message. For example, communication may be disconnected.

However, closer inspection of the entire disclosure of Roden reveals that the quoted passage has nothing whatsoever to do with periodically transmitting an encrypted key and then logging off a user when that user does not receive the key.

Instead, the portion of the specification of Roden upon which the rejections rely relates to "a method for allocating a cost associated with Internet access among the accessing end-user and Internet sides accessed by the end-user." (column 17, lines 25 – 28) Communications is disconnected when a message received by a credit server (which controls Internet access) does not include the correct key.

However, *Roden does not in any manner teach or suggest the claimed periodic transmission of an encrypted key, nor the claimed execution of a logout when the user processor in the receiver terminal does not receive the periodically distributed encryption key.*

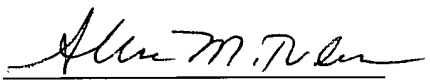
Roden discusses simply a well-known technique wherein disconnection is effected if the correct key is not received. **There is no disclosure at all of effecting logout upon the occurrence of *non-receipt* of a *periodically distributed* encryption key**.

Accordingly, the outstanding rejections are clearly not sustainable. As such, withdrawal of the rejections and allowance of this application are respectfully requested, and believed in order.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Allison M. Tulino
Registration No. 48,294

SUGHRUE MION, PLLC
Telephone: (650) 625-8100
Facsimile: (650) 625-8110

MOUNTAIN VIEW OFFICE
23493
CUSTOMER NUMBER

Date: July 20, 2005